AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

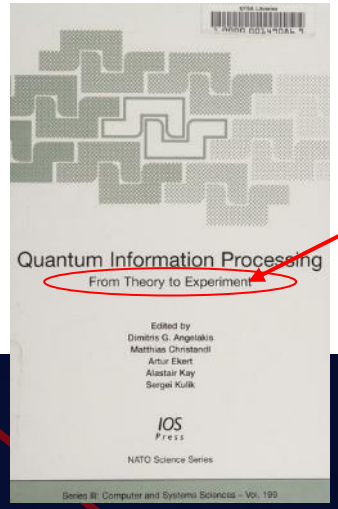
QUANTUM CRYPTOGRAPHY

Hannes Hübel
Senior Scientist, AIT Austrian Institute of Technology

3rd Training Event Hellas QCI, Heraklion (Crete)
4. 9. 2024

TRAINING IN CRETE?

2005: NATO Advanced Study Institute on Quantum Computation and Quantum Information



From Theory to Experiment

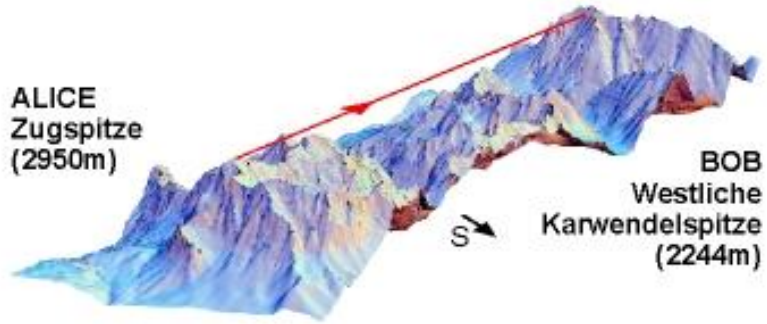
Chania

Heraklion

FIRST FIELD DEMOS OF QUANTUM INFORMATION APPLICATIONS

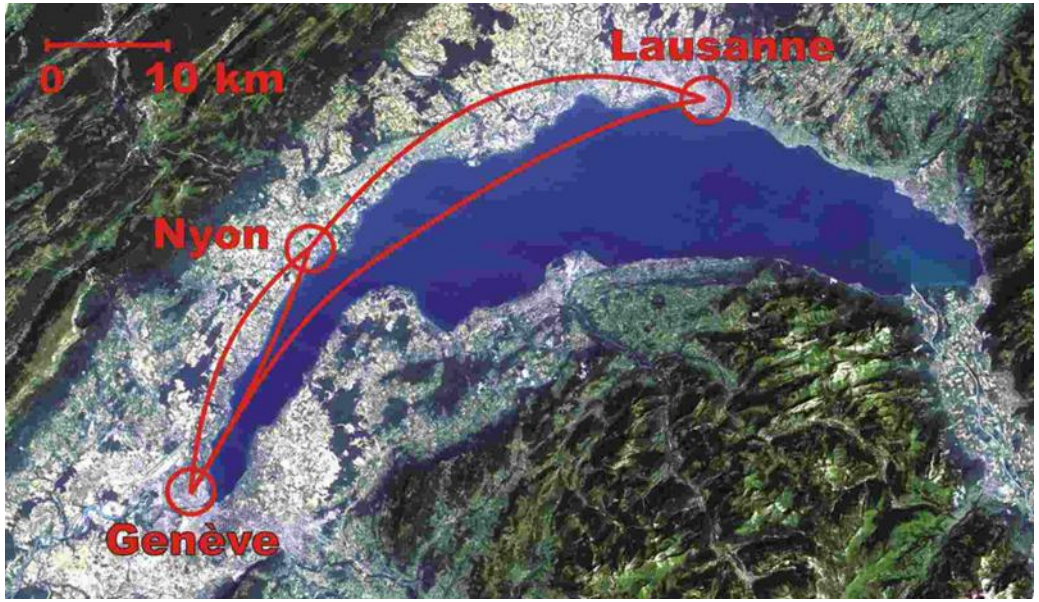
AUSTRIAN INSTITUTE OF TECHNOLOGY

Early 2000s



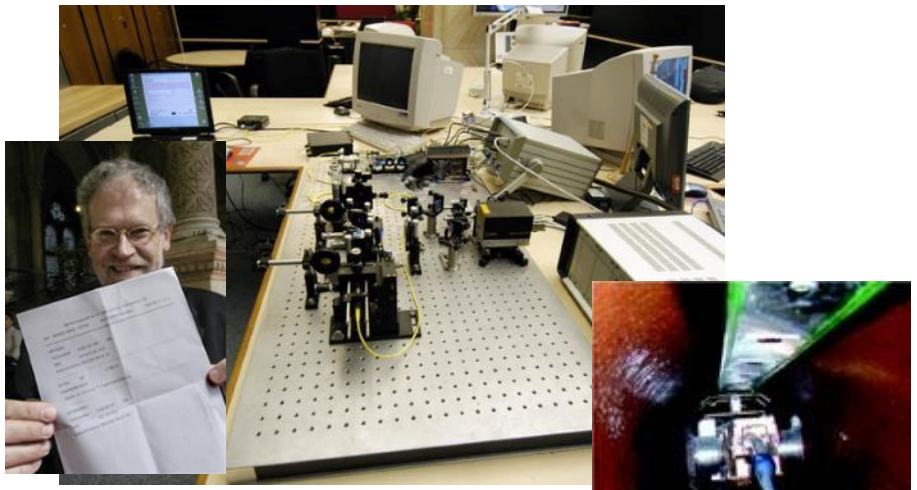
Nature 419 (2002), 450

2002 QKD; Distance 67km



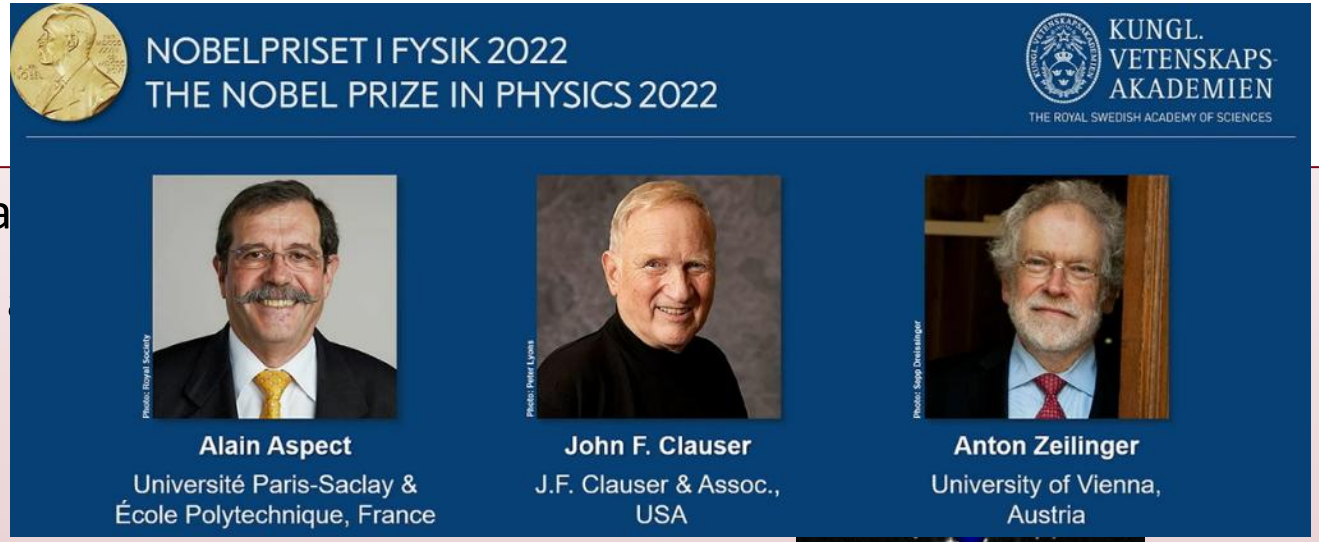
New Journal of Physics 4 (2002), 41.1

2004 QKD; Worlds first QKD-secured bank transaction



Opt. Express 12 (2004), 3865

TESTING THE LIMITS



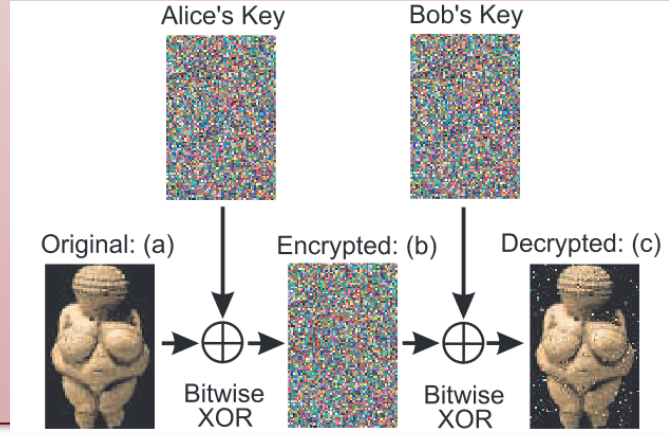
Quantum Communication field trials were motiva

- **Quantum entanglement** has no limits in time
- Einstein called it spooky action at a distance

Test at larger distances and faster speeds:

Phys. Rev. Lett. 81 (1998), 5039

Entanglement based QKD:



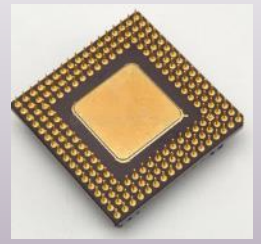
Phys. Rev. Lett. 84 (2000), 4729

QUANTUMTECHNOLOGIES

Do not undestimate the progress of technology

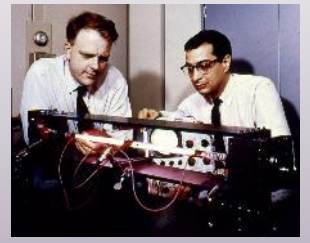
Computing power

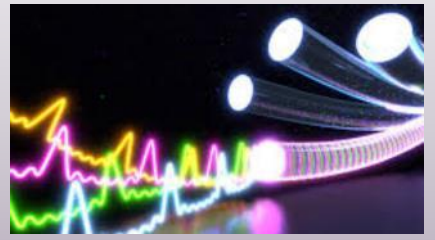
Semiconductor → Microprocessor



Connectivity

Laser → Optical communication



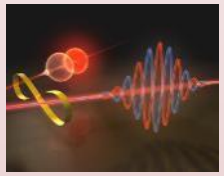
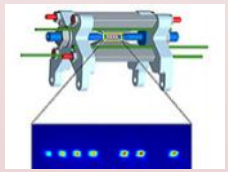
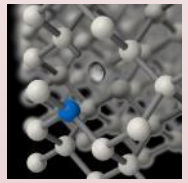
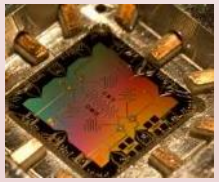
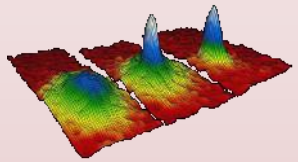


1st Quantum Revolution (1920 - 1960)

2ND QUANTUM REVOLUTION (1980 -)

Control over individual Quantum systems

- Photons, electrons, atoms, defects in crystals, etc.

- Quantum Systems can act as **information storage** and carrier
- Technological challenge: Creation, manipulation and detection of quantum states

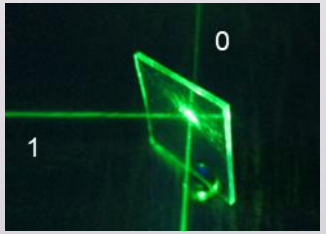
Quantum Technologies:

1) Quantum Computing
2) Quantum Communication
3) Quantum Sensing

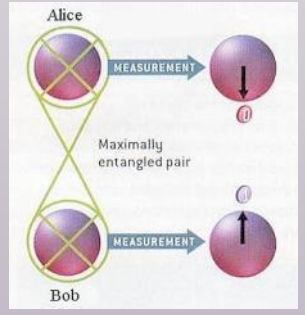
Differences to our classical world

Important quantum-physical phenomena:

- **Superposition**: 0 and 1 concurrently
  Quantum bit (Qubit)



- **No cloning:** Unknown quantum states cannot be copied with 100% certainty



- **Entanglement:**
  Correlated quantum randomness;
  Einstein: „spooky action at a distance“

QUANTEN COMPUTING

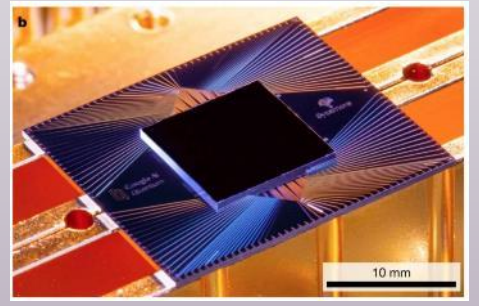
Quantum computers use the Qubit as processing unit.

- The Qubit can be in a state of „0“ and „1“ simultaneously.
- Strong **parallelisation of computation** possible -> find solutions that are too hard (in time) for classical computers

Application areas:

- Optimisation problems (e.g. logistics, Big Data, finance, forcasting, …)
- Chemical and biological reactions (e.g. pharmaceuticals, material science, catalysts)
- **Prime Factorization** (cracks currently used cryptography)
- Quantum Machine Learning
- …


IBM (US)



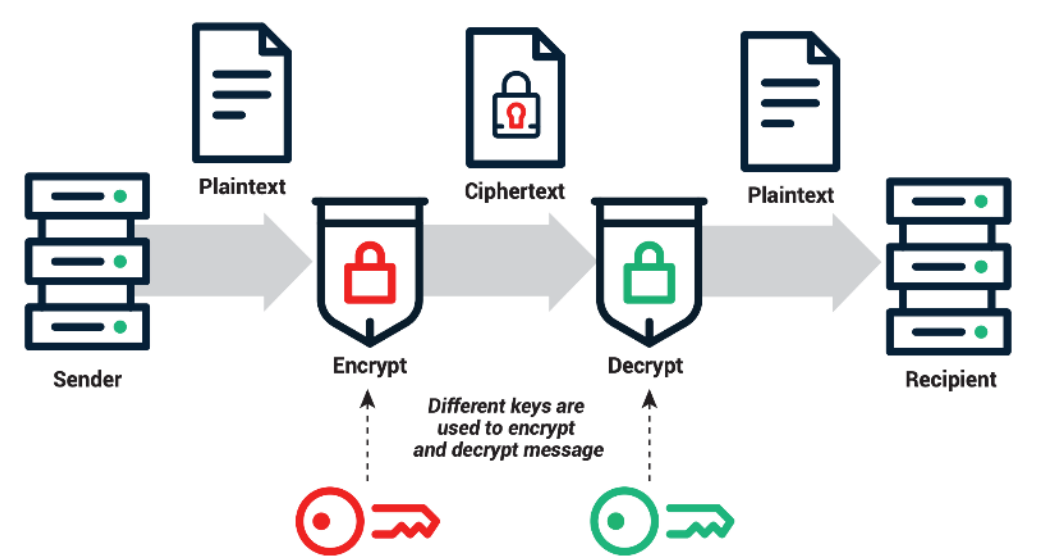
Google (US)

PASQAL (FR)


AQT (AT)

ASYMETRIC ENCRYPTION

Public Key Cryptography relies on computationally hard problems



Source: Sectigo

Public Key: $n = p \times q$

p and q are two large prime numbers; n is transmitted publicly to sender

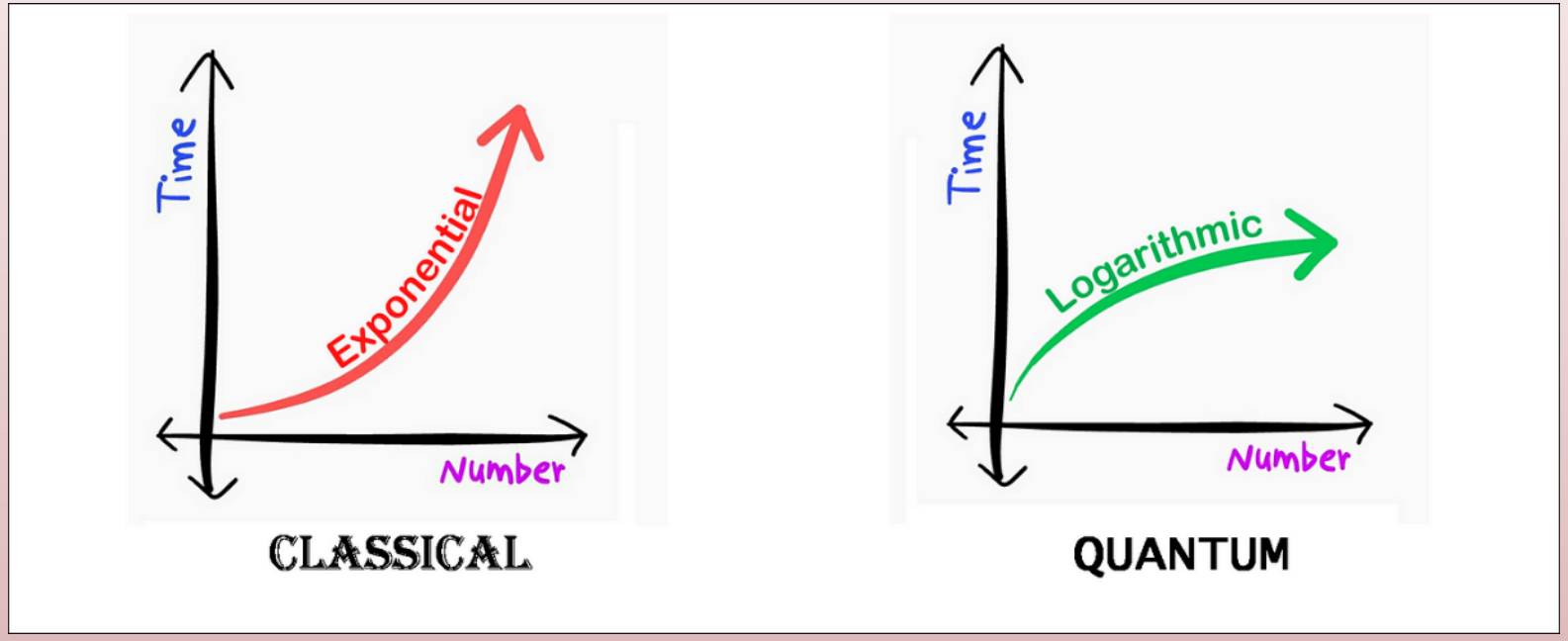
Private key: p, q

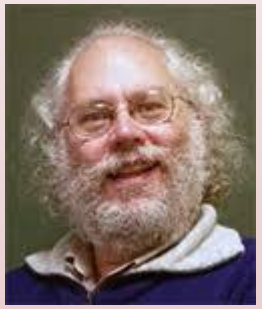
p and q are used to decrypt message

As long as p and q cannot be calculated from n, the procedure is safe.
Prime factorisation is (computationally) hard!

SHOR ALGORITHM FOR QUANTUM COMPUTERS

Developed in 1994, Shor's algorithm shows **exponential speed-up for prime factorisation**





P. Shor

What does it need to break a 2048-bit RSA encryption?

- **20.000 logical qubits (about 20 million pysical qubits)**
- **0.1% error probability**
- **8 hours**

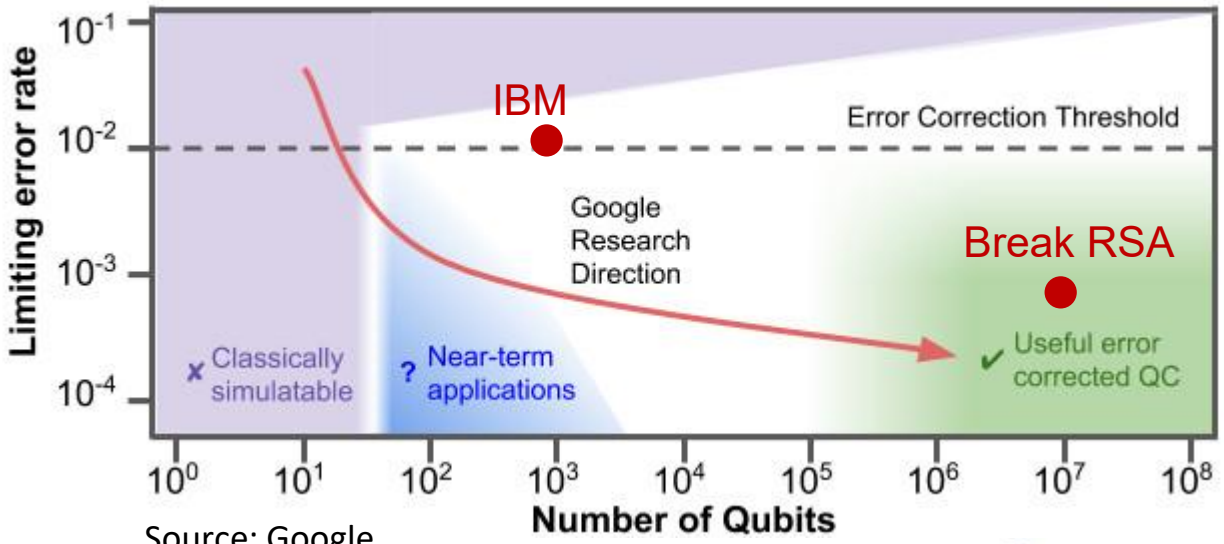
Quantum 5, 433 (2021)

RECENT PROGRESS

Many different Quantum computing companies on the market.

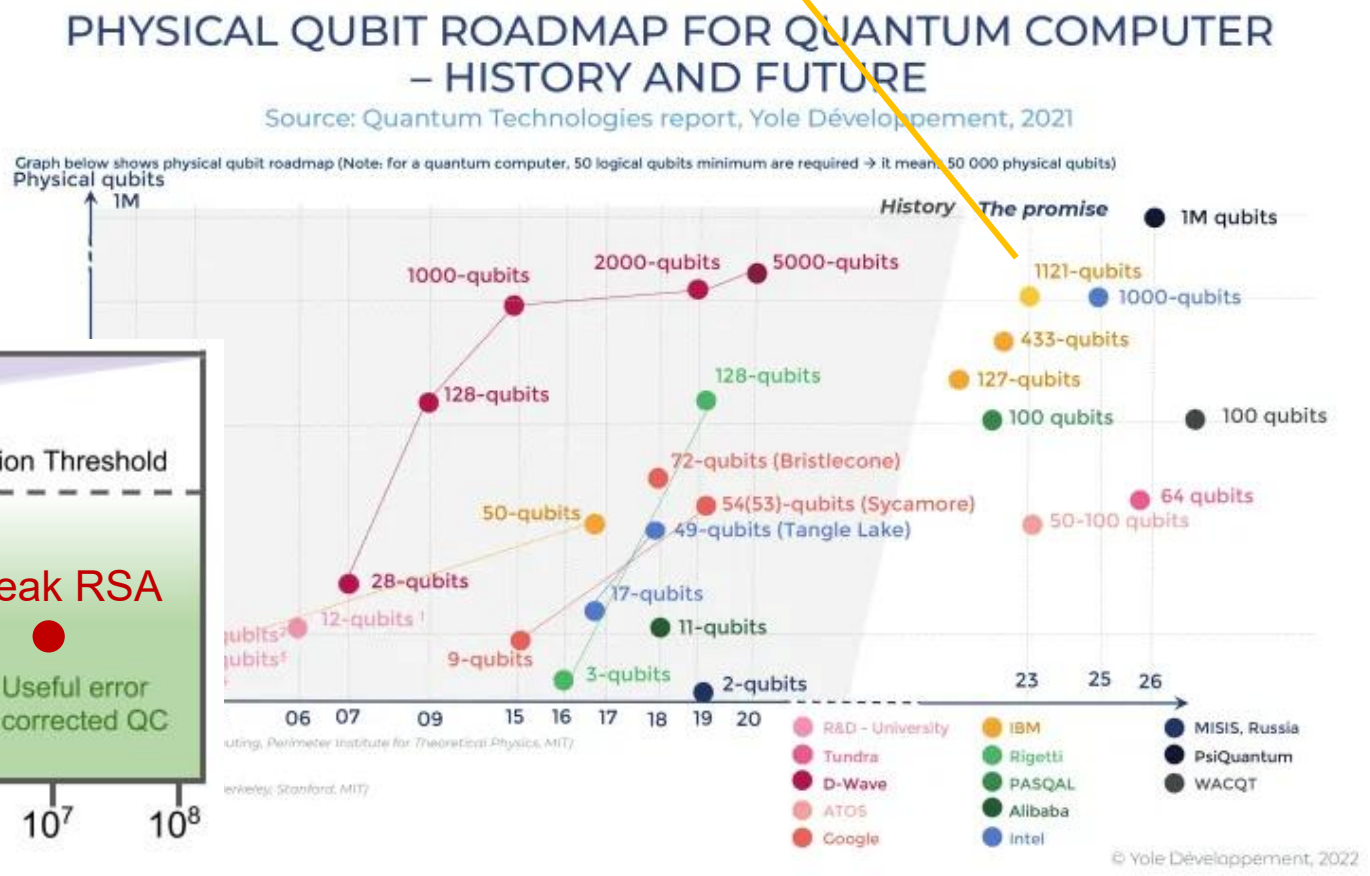
- Different physical realisation
- Current Qubit count between 20 and 1000

For real applications **millions of Qubits**



Source: Google

IBMs *1121 Qubit* chip in 2023



Source: YOLE

TIME TO ACT NOW

M. Mosca

Mosca's Theorem:

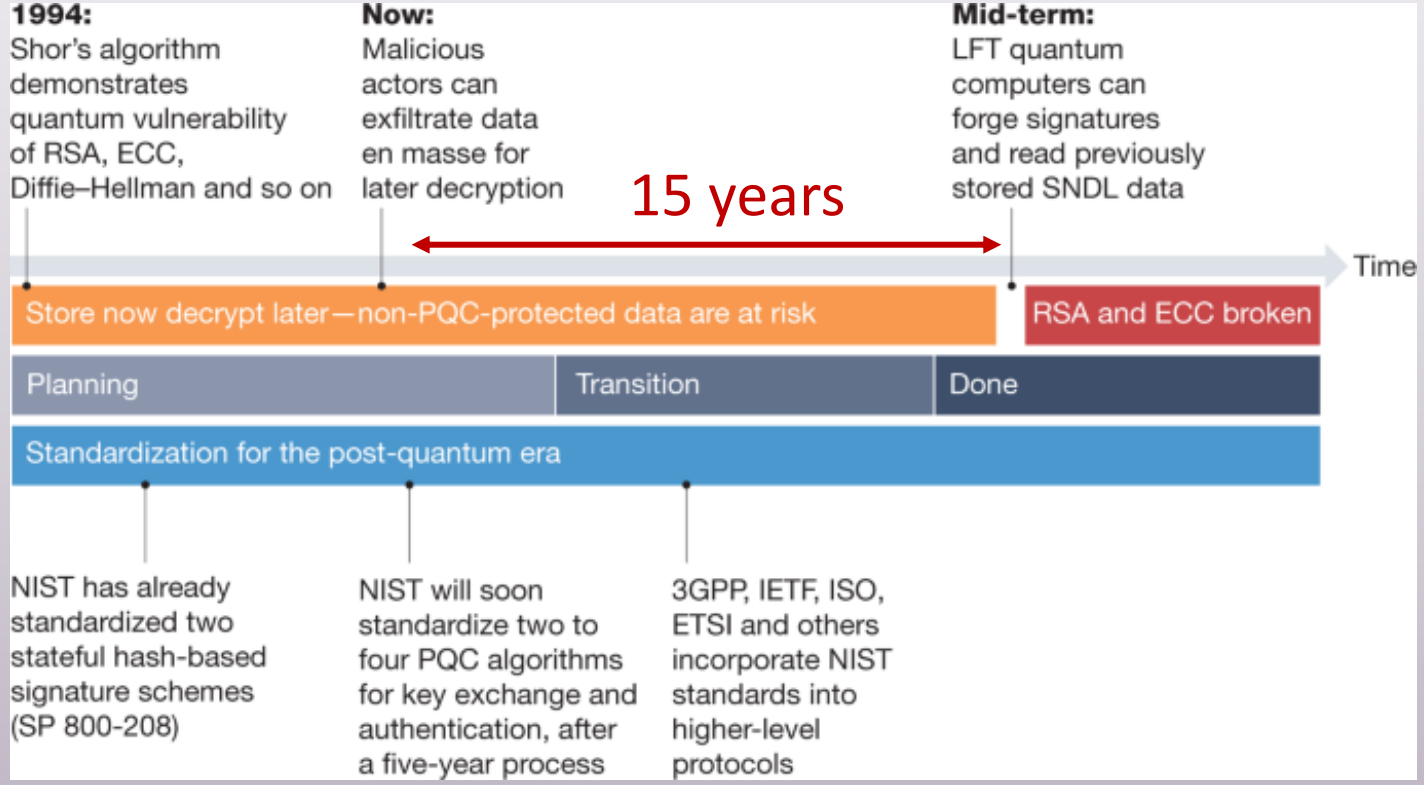
Lifetime of secret + Migration time > Development of useful Quantum Computers

If this is true, you are in trouble…

POST-QUANTUM CRYPTOGRAPHY

Post-Quantum Cryptography Standardization programme launched by NIST in 2016

PQC transition roadmap:



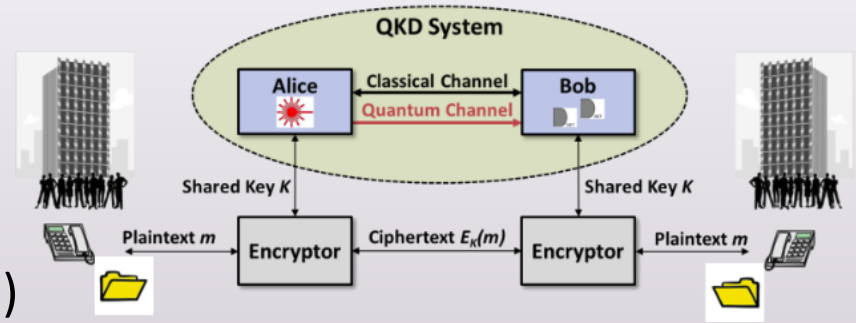
Nature volume 605, pages 237–243 (2022)

QUANTUM COMMUNICATION

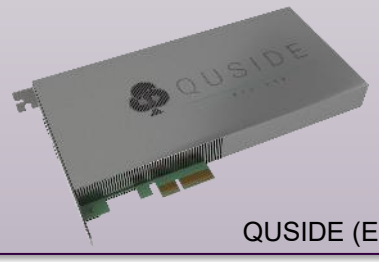
Quantum communication allows **exchange of classical and quantum information**.
Information carrier: **Qubits (primarily photons)**
Quantum mechanics guarantees that the exchange of information is **absolute secure**. Secure against all classical and quantum attacks.

Application areas:

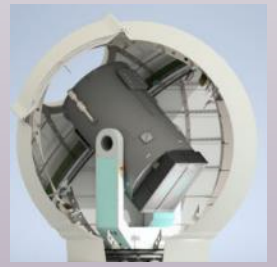
- **Secure key exchange – quantum key distribution (QKD)**
  - Distribution of symmetric keys
- Quantum random number generator – QRNG
- Multi-partite computation (e.g. secret sharing, oblivious transfer,…)
- Quantum Teleportation and Quantum Repeater
  - Quantum Internet linking distributed quantum computers and sensors

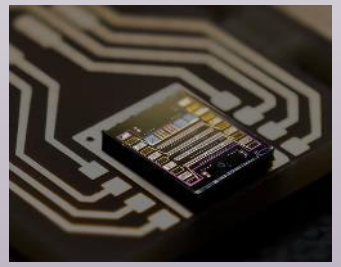


Think Quantum (IT)



QUSIDE (ES)


QTLabs (AT)


Sparrow Quantum (DK)

ADVANTAGES OF QKD

Long-term Security

- Forward secrecy
- Guaranteed safety for decades
- Medical and biometric data

ITS – secure Encryption

- Combination of QKD and one-time pad
- Governments
- Military
- Critical infrastructure

Dynamic Keys

- Fast renewal of keys
- 64GB[1] of AES encryption per key
- Crypto agility

[1] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf

ADVANTAGES OF QKD

Long-term Security

- Forward secrecy
- Guaranteed safety for decades
- Medical and biometric data

ITS – secure Encryption

- Combination of QKD and one-time pad
- **Governments**
- Military
- Critical infrastructure

Dynamic Keys

- Fast renewal of keys
- 64GB[1] of AES encryption per key
- Crypto agility

[1] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf

EUROQCI

- An **integrated satellite and terrestrial system** spanning the whole EU for **ultra-secure exchange** of cryptographic keys (Quantum Key Distribution)
- Quantum communication infrastructure (QCI) is part of the **European Cybersecurity Strategy** and is to be integrated in the new Secure Space Connectivity initiative 'IRIS²'

EuroQCI space segment
Distribution of quantum-secured encryption keys on a global scale

EuroQCI terrestrial segment
Federation of national terrestrial QCI networks with cross borders connections

EUROQCI TIMELINE

2020 24 25 26 27 28 29 30

Studies
- Design & architecture

DEP projects

Preparatory and first deployment phase
- Establishing first national networks to experiment with QKD technology

DEP projects (2nd phase) and CEF-II

Operational deployment phase
- Operational deployment
- testing, validation and operationalisation
- cross border links

Full operation

EuroQCI

Eagle 1 – First in orbit demonstration

Launch

Operations (IOV)

SAGA mission

Operations

TECHNOLOGY

Advanced **QKD ecosystem** in Europe

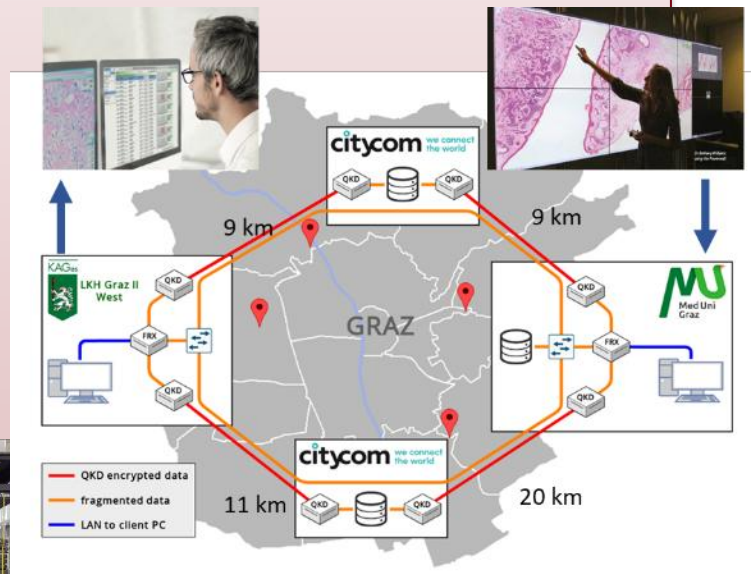
- **Component** suppliers
  - QKD-grade lasers, modulators, detectors
- QKD **system manufacturers**
  - High TRL, ready for deployment

- **Key management** system providers
  - Build large networks with end-to-end encryption
- **QKD-ready encryption** devices
  - Seamless integration into existing communication networks

USES CASES

QKD demonstration for medical uses-case

Secure storage and retrieval of medical data



Deployed QKD network in Graz (Austria)

Dry-run of optical network

Players:

End-users and service providers:

- Medical University and local hospital
- Data center provider (CityCom)

Infrastructure provider:

- 2 Data Centers
- 4 fiber links (9 – 20 km)

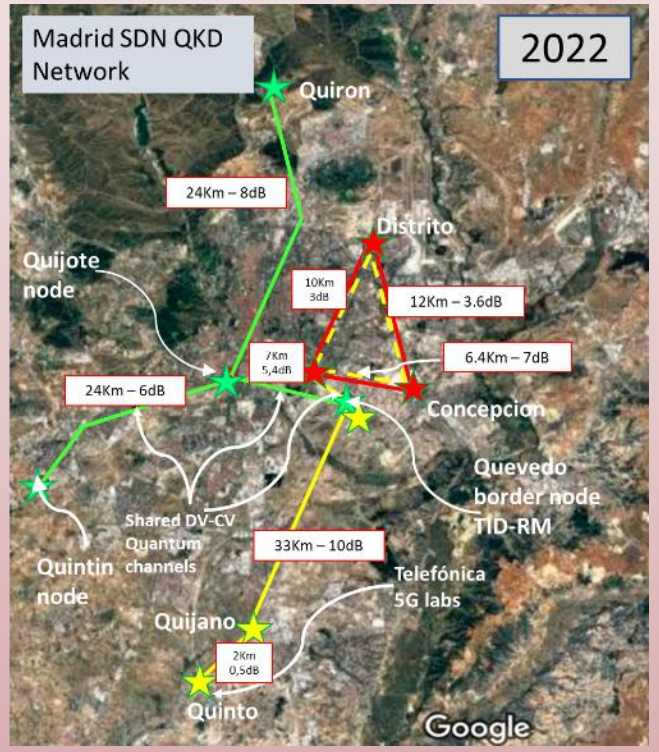
Device manufacturers:

- 4 QKD links (IDQ)
- 4 pairs of layer-2 encrytors (ADVA)
- 2 secret sharing devices (fragmentiX)

NETWORK DEPLOYMENTS

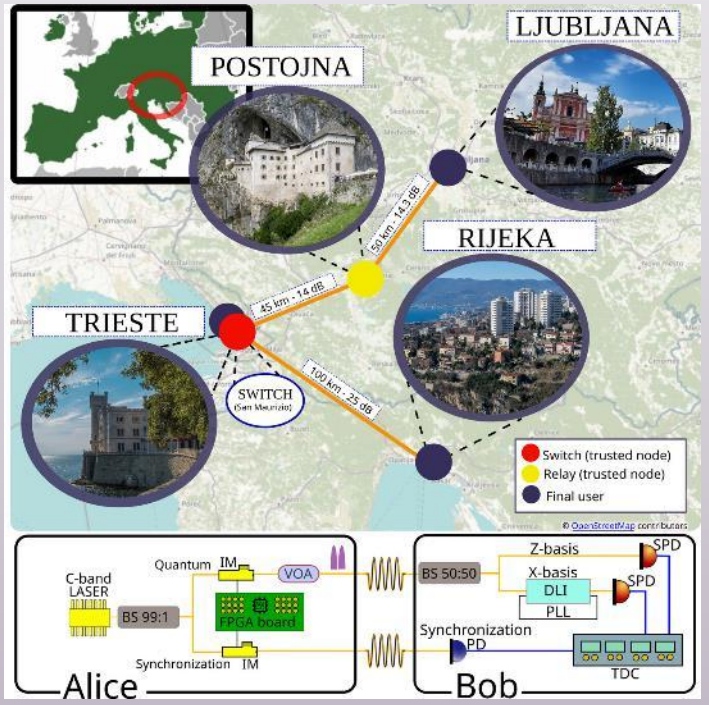
Large **QKD deployment** in Madrid

- Use of Telefonica network
- 10 nodes
- 13 QKD links
- 7 Link encryptors



Cross-border demonstration Italy – Slovenia – Croatia

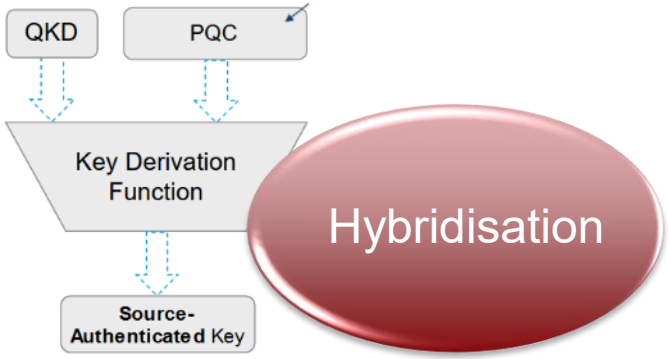
- 200 km network
- 4 nodes
- 3 QKD links
- KMS layer
- Securing of VPN connection



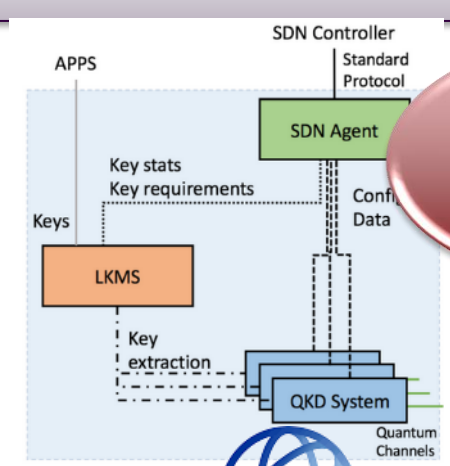
Adv Quantum Technol. 2023, 6, 2200061

WHAT MORE IS NEEDED

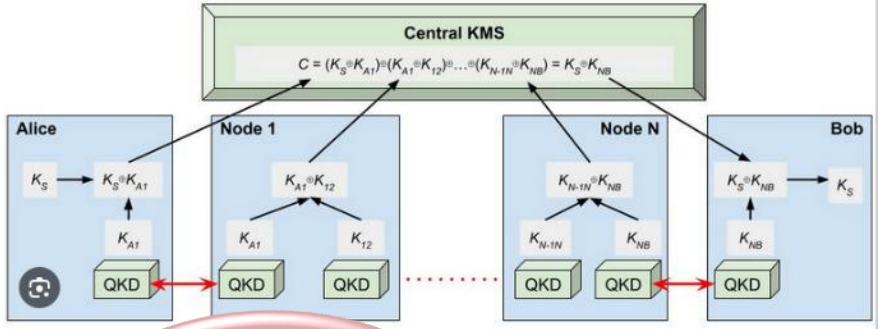
Fully operational EuroQCI



Hybridisation



SDN functionality

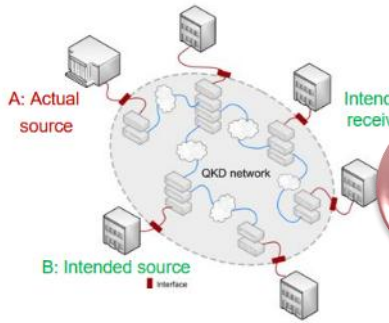


Key forwarding

EuroQCI

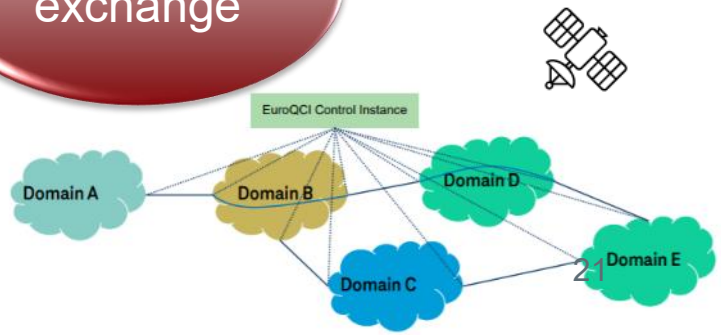
Certification

N STRADAMUS



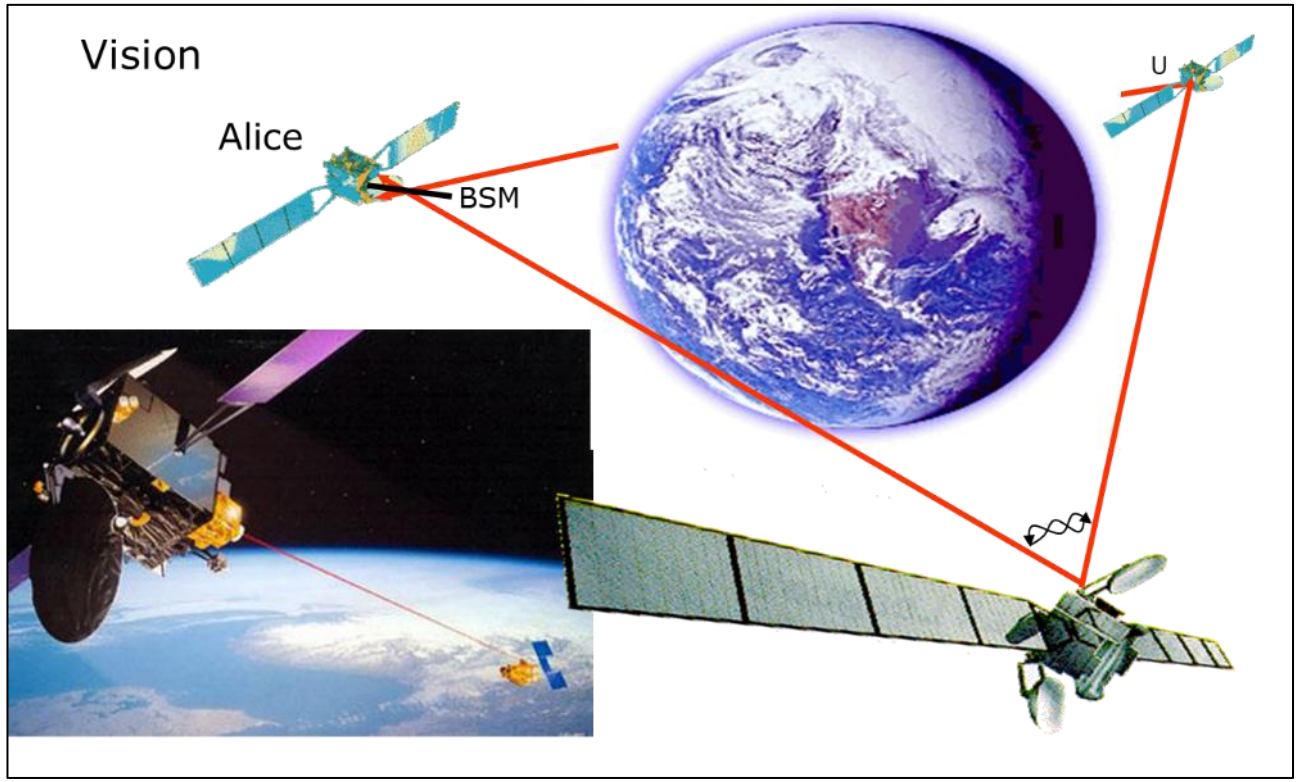
Authentication

Domain exchange



VISIONS

Last slide from my talk in 2005 in workshop on Crete:

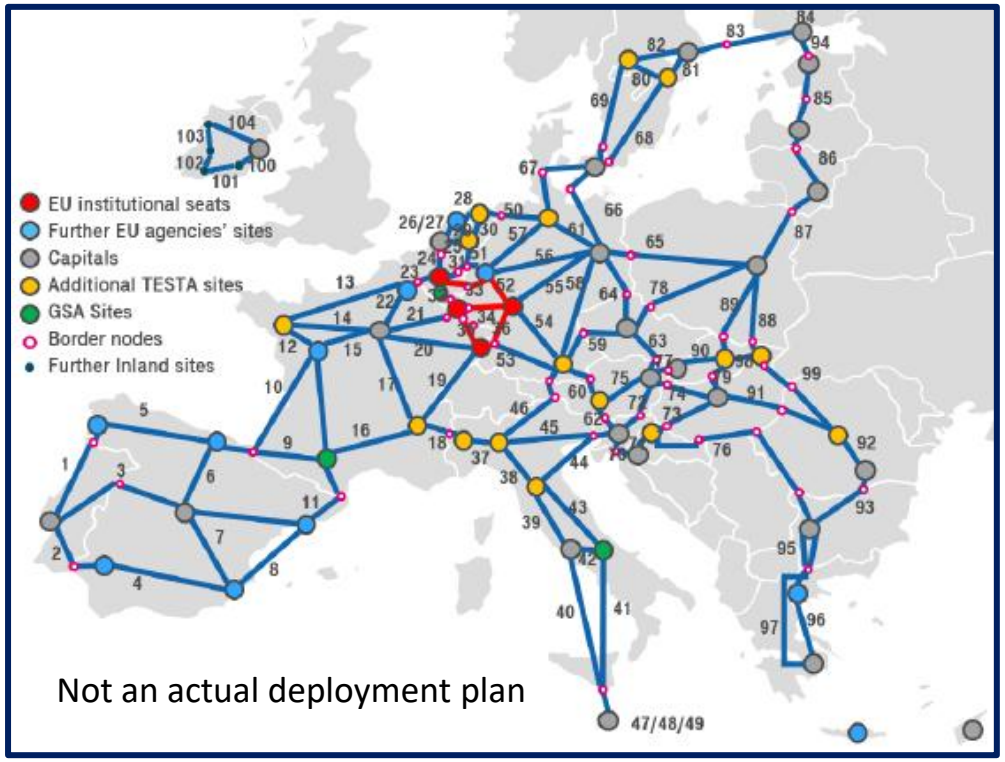


… became reality in 2017

First European QKD satellite (QUBE) was launched in August 2024

VISIONS

Confident that by 2035 there will be an operational pan-European QKD network !



maybe even more general quantum communication networks with applications beyond QKD

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

MANY THANKS!

Hannes Hübel

hannes.huebel@ait.ac.at